PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 :
G06F 12/14, 12/16

A1

(11) International Publication Number: WO 93/09498

(43) International Publication Date: 13 May 1993 (13.05.93)

(21) International Application Number: PCT/KR92/00053

(22) International Filing Date: 28 October 1992 (28.10.92)

(30) Priority data:
PK 9130 28 October 1991 (28.10.91) AU

(71)(72) Applicant and Inventor: YANG, Sung, Moo [KR/KR]; 510-8 (16/6), Shinlim-4-dong, Kwanack-gu, Seoul 151-014 (KR).

(81) Designated States: AU, CA, GB, JP, KR, US.

Published
With international search report.

(54) Title: METHOD AND SYSTEM PROTECTING DATA IN STORAGE DEVICE AGAINST COMPUTER VIRUSES

(57) Abstract

The present invention provides a protection that protects resources in storage device against computer viruses. Storage device are used to store or retrieve data by computer but computer viruses access the resource in the storage device and even damage data. This invention embedded in controller of storage device, main system or operating system probes write operation to storage device and determines whether legitimate or illegitimate operation. Privileged signal is used to authorize some operations is only derived from keyboard stroke or other switch device not from process. Gate system forwards data to be written to storage device if the proposed operation was legitimate otherwise the data is not forwarded.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria
AU	Australia
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CS	Czechoslovakia
CZ	Czech Republic
DE	Germany
DK	Denmark
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IT	Italy
JP	Japan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakhstan
LI	Liechtenstein
LK	Sri Lanka
LU	Luxembourg
MC	Monaco
MG	Madagascar
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SK	Slovak Republic
SN	Senegal
SU	Soviet Union
TD	Chad
TG	Togo
UA	Ukraine
US	United States of America
VN	Viet Nam

METHOD AND SYSTEM PROTECTING DATA IN STORAGE DEVICE AGAINST COMPUTER VIRUSES

Field of the Invention

This Invention relates to the computer viruses and more specifically to protect computer data on storage device against computer viruses.

Background Art

A well known computer virus in IBM PC environment would be Brain virus, the named derived from volume label. The virus infects boot sector of disk or diskette and resets volume label as "(C)Brain". The virus has few editions some of the virus reside on data area(DA) of diskette, which was not used by system, and resets File Allocation Table(FAT) in disk as 'bad cluster'. FAT is a system area in disk or diskette formatted under DOS operation system, containing file allocated information on disk represented by linked list structure.

A virus that resides on boot sector of disk or diskette and takes control when system is booted. The virus may stay in memory, which is called Terminate and Stay Resident(TSR) program, until power is down. Another well known type of virus resides in a binary file . The virus is active when a program that virus resides in is invoked. The virus became active entity and find not infected binary file and infects other binary files. Virus achieves goal of propagation itself by infection

procedure. The infection procedure makes a binary file infected program.

Virus instructions are usually machine instructions of target computer but rarely and possibly shell program(batch file program) can also contain virus code.

Virus intrinsically propagate itself and became many in number. Virus also to be increased by copying an infected software by users. Virus is also increased by a person who put virus code into system deliberately or unintentionally.

A manner of activity while staying memory, on DOS, is reported that virus code typically changes interrupt vector of INT 21H (decimal is 33) and some other interrupt vectors to itself°so that when interrupt 21H is occurred virus instructions are executed. Virus can do variety of task at this occasion, for example, propagate, display a message, destroy, modify data in storage, modify data in memory etc, and the virus sends control to original interrupt service routine. Any operation seems like normal but the RAM resident portion. User might believe and the data in disk is safe and correct while data has been or will be altered.

Several kinds of effort have been made to cure against threatening of virus. Password, check sum, encryption, scanning and elimination and alert technique. Law enforcement.

Well organized access system may help to protect system from virus

Binary files are altered while it is not necessary, and data files are modified by any program(process) not necessarily. Well known personal computer under DOS doesn't provide level or mode of process. Any process potentially can access any resource without restriction under DOS while other operating systems do provide access rights, for example a well known operating system UNIX. Normally process in kernel mode(or monitor mode) has privilege and can access any resources without restriction while process in user mode is restricted to its area in accessing resource. If virus has the privilege which is kernel mode, it would be dangerous. Virus potentially can reach high or the highest level. Herein, the invention provides a privileged signal which ever existed. Virus cannot reach the level of privilege named Keyboard Privilege(KP). This will task a fundamental role of this invention. As a result, this invention enables a system that never virus to reside. Virus can be defeated by not to allow space to reside in computer storage system while virus needs a space, which is non-volatile storage, to reside.

Infection is done by four different ways. One is that, we are concerning, propagation, which is done by virus itself and intrinsically character of virus. Virus must alter binary files or some of system area where virus can reside on. This invention can prohibit alternation to

binary files or some of system area. For example, when computer virus attempts to alter a binary file that has been locked by user, this invention rejects the attempt without any interference with other system.

While binary files that have been locked are protected and never be altered, compiler and linker wouldn't work properly. This problem is concerned and solved by policy of association.

A sort of virus may reside on boot sector of boot sector, which is located the first sector of each disk/diskette. This attempt is also rejected.

Concerning data file, viruses may attack to data files or alter some of data. This is also prevented without interference. A remedy named association that gives authority to specific application programs. In conventional system, the access right was opened to any process, while it was not necessary.

Brief Description of Drawings

Figure 1 depicts conventional system in which disk controller connected to disk drive. Figure 2 depicts an implementation embedded in disk controller. 1 is this invention comprising disk controller. Figure 3 depicts a path for privileged signal, which is a jumper line 2 between keyboard connector and this invention 3 embedded in a disk controller, peripheral device.

Brief Description of Invention

This invention consists of Decision making system, Gate system.

Decision system makes decision whether opening the gate or not. Gate mechanism controls flow of data to be written on storage device.

This invention restricts illegitimate write access to resources in storage device including disk drive, floppy tape, optical drive, RAM drive. This invention provides the most effective protection against computer viruses. Let user confine accessibility given to conventional system. A specific file or a group of files are prohibited from alternation even in kernel mode.

Decision making and gate system that embedded in conventional system. Decision making system exams all write operations whether legitimate or not; since virus can manipulate files on storage device, this probe is necessarily required for safety. If a result of probe is legitimate, this let gate open otherwise let close.

This invention makes decision according to policy of Association and Isolation. The policy of Association (referred to Association) confines program's access right into a specified group of data files. The group is represented by extension, which is a part/suffix of file name and denotes file type. The policy of Isolation (referred to Isolation) restricts write access to some object(files), which is in LK state. All the restrictions

are devised in the interest of security against computer viruses.

Gate embedded in conventional system and rejects a write operation proposed when gate control command was NOPEN so that the data to be written on storage device is not forwarded . and doesn't rejects the proposed write operation when gate control command was OPEN.

This invention support a special case that compiler or linker produce files in state LK(read only mode) to prevent possible infection from computer viruses. This invention gives compiler and linker an exception when they overwrite on binary files they have produced before.

Detailed Description of Invention

This invention consists of policy and mechanism carries the policy.

This invention has equal application to any type of computer system that comprises storage device. This invention has equal application to any type of storage device. For example, the present invention is not limited to hard storage device but has application to optical, floppy, tape, RAM drive and other storage device as well. This invention can be implemented by a peripheral card or software embedded in system kernel.

Although this invention should be implemented by hardware, it may be also implemented by software. When a target computer in which this invention is intended to implement comprises the memory protection facility, this invention can be implemented by software and would be effective as much as hardware implementation except some cases under special circumstance. For example, this invention may not work accordingly as this invention was intended if some of a portion of its software is altered. This alternation can be possibly occurred by virus or some other reasons. An advantage of hardware implementation is high reliability and an advantage of software implementation is cheap cost of implementation.

A computer system without memory protection facility must be chosen hardware implementation for reliability

When this invention is implemented by hardware, this may be embedded in peripheral device, referring Figure 2. When this invention is implemented by software, this may be embedded in Kernel of Operating System.

A write operation may be driven by computer virus, if the system is under control of virus. This invention embedded on conventional system and exams all the write operations before they are written. This invention make decision whether approve write operation or not according to this invention's policy.

There are some fundamental functions used in decision making system. GET_CAP(Currently Active Program) gets the current active program in system, GET_CBHF(Currently Being Handled File) gets the currently being handled file, GET_CBHFE(Currently Being Handled File's extension), GET_TRANSIT gets a transit and FindCase matches the currently active program and the currently being handled file with a case.

Decision making system is depicted clearly and simply by a pseudo code like C computer programming language.

```
decision()
{
        if((FindCase(LC)==LC1)    return OPEN;
        if (FindCase(A)==A2)      return NOPEN;

        c=FindCase(I);
        if (c==I1,I2,I3 or I4)    return OPEN;
        if (c==I5 or I6)          return NOPEN;

        c=FindCase(K);
        if (c==K1)                return OPEN;
        if (c==K2)                return NOPEN;
        } /* decision */
```

FindCase(LC) attempts to match currently active program(CAP), which would be compiler or linker, and

currently being handled file(CBHF) with cases from LC1 to LC3.

Case LC1 is defined that CAP (currently active program) is found and is associated with CBHF(currently being handled file) in table ADLC. Case LC2 is defined that CAP is found and is not associated with a CBHF in table ADLC. Case LC3 is define that CBHF is not found in table ADLC. These may be abridged as following:

Case	CAP is		Decision
LC1	found	associated with CBHF	OPEN
LC2	found	not associated with CBHF	NOT OPEN
LC3	not found		NOT OPEN

If case LC1 is matched with CAP and CBHF, decision is made as OPEN otherwise CAP and CBHF are attempted to match with case between A1 and A3.

Case A1 is defined that currently being handled file's extension(CBHFE) is found and is associated with CAP, which would be an application program, in table ODT. Case A2 is defined that CBHFE is found and is not associated with CAP in table ODT. Case A3 is defined that CBHFE is not found in table ODT. These may be abridged as following:

Case	CBHFE is		Decision
A1	found	associated with CAP	NOT DECIDED
A2	found	not associated CAP	NOT OPEN
A3	not found		NOT DECIDED

If matched with a case A2, decision is made as NOT OPEN otherwise another attempt is made. FindCase(I) attempt to match a case between I1 to I4 with CBHF.

Case I1 is defined that transit is p1, r3, p4 or p5. Case I2 is defined that transit is r2 or r6. Case I3 is defined that transit is q1, q4 or q5. These may be abridged as following:

Case	Transit	Decision
I1	p1,r3,p4,p5	OPEN
I2	r2,r6	NOT OPEN
I3	q1,q4,q5	NOT DECIDED

If matched I1, I2, I3 or I4, decision is made as OPEN, if match I5 or I6, decision is made as NOT OPEN otherwise next attempt is made. Finally, there are two case P1 and P2 so that matching is finalized though no match was done so far.

Case P1 is defined that privileged signal is issued to approve proposal. Case P2 is defined that privileged signal is not issued or issued to disapprove. These may be abridged as following:

Case	PS	Decision
P1	APPROVAL	OPEN
P2	DISAPPROVAL	NOT OPEN

A proposed write operation is described by EXTid, PGid, Ofi that represent current situation. Ofi is represent a file is in storage device, is used as a

identification to files. PGid is an identification to programs, in a storage device. LCid is an identification to linker and compiler, used to identify compiler or linker from other linkers or compilers. EXTid is a identification to extensions of a file name. A file in a storage device may be referred by Ofi, PGid, EXTid and LCid.

After decision making process is ended, a command is passed to gate system. The command will be either OPEN or NOPEN. The command OPEN means gate let requested data forward storage and the command NOPEN means that gate doesn't let requested data forward storage but resumed.

NOCOMMAND is used to indicate initialized state.

Gate Control Commands

-NOCOMMAND

-OPEN

-NOPEN (do not open gate(reject) and resume)

-NOPEN2 (reject and generate error)

There are four of states object(file) can be. State UK in which object is accessed to write. State LK in which object is accessed only to read, write access is forbidden. State AL in which object is alerted. State WA in which object is being altered.

Isolation prohibits write access to locked object, which is in LK state. Conventional system doesn't provide strict and proper restriction to those that are in state

LK while this invention distinguishes them and restricts write operations to locked object.

Isolation isolates binary files that you want from alternation. Object in AL, LK states should be isolated, and LK shouldn't be altered. More specifically, PS(privileged signal) enables files in state LK, AL to be state UK.

More specifically, object can have state WA, UK, LK and AL. According to policy of isolation locked object can't be altered. If data was destined to write on locked object, this operation is ignored and result of record is remained in 9134.log. If data was destined to write on alert object, this operation caused confirmation/asking message window will be opened. If data is destined to write on unlocked object, this operation is granted. Isolation shouldn't interfere with conventional system. The policy should not be violated.

A mechanism of association is designed to find out relationship between program(data file handler) and data file. A table named ODT contains all relationship between them.

EXTid field	Program field
EXTid	PGid...

User can change these descriptions by editing ODT.DSC. A group of data files are specified in the table and its handlers are specified right-hand side of table while data files are specified left-hand side. This table is

referred by decision making system A specified group of data files are only allowed for write access by the specified handlers. Additionally this table may contain linker and compiler on the program field when EXTid is 255.

A mechanism of isolation is design to exam write operations. This refers BMT to know a state of object and reports 'illegal operation' when a write access was made to object in LK state. The table contains all the state of each object and maintained accordingly changes.

Unlocking and disabling alert operations require privileged signal to cope the demands otherwise the demands won't be able to cope.

Demands	Meaning
DU	Demand of unlocking
DS	Demand of suspending alert
DD	Demand of disabling alert
DC	Demand of Configuration Setting
DR	Demand of Reallocation
Dds	Demand of Disable
Den	Demand of Enable
Dupg	Demand of Upgrade
Ddt	Demand of upgrade table
Dbt	Demand of boot sector

Any illegal operation found by Decision Making System doesn't reported immediately but recorded into a file

9134.LOG reserved in a mass storage device with some related information. This illegal operation causes system not to be affected and system will be able to resume next task.

To recognize virus and legitimate commands are not easy task. A privileged signal may be used to approve or authorize an operation or command as means of reliably distinguish virus and user. For example, if a signal, privileged and virus can't issue or alter, is used when an important operation is proposed or requested. Computer system will not be confused.

Isolation's policy definitely requires privileged signal (PS) when unlocking, disabling and alert. Fortunately unlocking locked file would be a rare operation. User may user this command when remove a program that had been locked in their hard drives or floppy disk drives. Unlocking operation is not special command in system because the operation is exactly same effect with read only attribute set or

chmode u-w or

chmode g-w or

chmode o-w or

chmode a-w

To implement issuing Keyboard privilege require simple hardware circuit than software because if software can issue PS, it means that virus also can. The issuing PS

caused user shouldn't be bothered. This invention provide a privilege that derive from physical action not from process.

A keyboard signal is used as privileged signal in an embodiment of present invention. Keyboard is connected with an IO port on system. CPU gets a word or byte from the IO port as means of read keyboard scan code. This invention gets a signal directly from the IO port as means of fetching privileged signal. Alternatively, this invention gets signal directly from the keyboard connector by a jumper line between this invention and keyboard connector.

The keyboard privilege can not be violated by any process like virus because it is issued by pressing keyboard or specially designed to issue approval. The privileged signal may be simulated or imitated by no other process or executable code or instruction. Since signal is only derived from by the keystroke, no other generate the signal. It may be generated by a bug on keyboard circuit. This invention assume that system have no such a bug and computer circuit was designed that keyboard scan code is delivered to IO port and no other process can generate the signal except keyboard.

So far any resource can be control by a process but this invention provide a level of privilege that virus can't reach.

When this invention is embodied, some matters should be satisfied in the interest of reliability. Write probe mechanism exams a block of data requested to write in Decision making system. The write probe mechanism should be placed before proceeding write operation and before gate mechanism.

Gate mechanism must place before writing on storage device

Gate mechanism is recommended to nearest to the storage device. Gate and write probe mechanisms may be placed together and gate shouldn't be malfunctioned or by-passed. It means that after gate mechanism, no interference is allowed. An embodiment in which the gate is a hardware, which is embedded in storage device as part of the storage, so that no process and executable code can effect operation of the gate and placed the adjacent to hard drive; connected to directly as hard disk interface or hard drive controller- would be ideal. All these arrangement are made to get rid of possibility of illegal alternation to data after gate system.

Compiler and linker should be able to produce binary files and overwrite them. To overwrite binary files are usual transaction but this should be able to do. Compiler and linker support mode provide a special function that any binary files(BFA) produced by a compiler or linker can be overwritten by the compiler or linker, no matter BFA is locked or not.

Concerning compiler or linker is needed in this because compiler or linker may produce files in LK. In this invention compiler and linker can produce files without any restriction while other program can not. When compiler and linker produce files BFA(Binary Files to be Altered), this invention adds items into table ADLC. When compiler and linker produce another file that doesn't exist also to be added into ADLC table. It is like following:

Linker or Compiler field	BFA field
LCid	Ofi ...

This invention probes accessibility of writing, before compiler and linker produce/overwrite files. If access was legalized, the operation is done, otherwise the operation is denied. When compiler or linker produced files that do not exist currently in system or exist and in UK state, this operation is done and item is added in table ADLC if the file is not existed in the table.

This has a facility to reallocate files in storage device. This is performed to increase access efficiency, is not possible.

Descriptors exist in storage device. ODF.DSC UPGRD.DSC and EL.DSC are those files. These files contains information on association between object(files) and program. EL.DSC contains extentions is optionally used. ODF.DSC is edited by user. EL.DSC can be edited by user.

Both of files are not to be removed and in AL state. If the files were damaged or removed caused by any accident, they are recovered by system. Any alternation, remove or append an item, causes system opens and reads the files. These files are edited by editor DSCED. UPGRD.DSC is given by dealer, containing new information. This is used when system upgrade.

An Embodiment of Present Invention 1

This emulate this invention. This is designed to work under DOS environment without any hardware support so that it doesn't have reliable protection and can't demonstrate all the feature of this invention.

Primary Modules and Mechanism

Decision

Maintenance

Gate

Diagnosis

Privileged Signal Handler

Memory

IO

Debug

An Embodiment of Present Invention 2

An Embodiment of Present Invention is a hard drive interface card, which is connected to directly hard drive. No process or executable code can interfere, so that the highest privileged mechanism is realized.

All the mechanisms of gate and decision making system are comprised within the card.

An Embodiment of Present Invention 3

This is embedded in a system kernel. The mechanism doesn't have the highest privilege as this invention should have but this was is cheap way to implement.

CLAIMS

1. A method protecting resource in storage device against computer viruses comprising:

initializing;

determining whether proposed write operation is legitimate or illegitimate based on a currently active linker program, compiler program, a currently active application program, a currently being handled file, associated information or mode of a current being handled file;

rejecting said proposed write operation if said proposed write operation is not legitimate;

forwarding said proposed write operation to storage device if said proposed write operation is legitimate;

reallocating contents of files in order to optimize access time to storage device;

attempting to recover faults occurred in conventional system;

diagnosing integrity of system;

disabling determining.

2. The method of claim 1 wherein said tables are built by a initializing program;

said tables comprising ADLC, ODT, BMT and EL.

3. The method of claim 1 wherein the method of determining comprises the steps of:

probing said proposed write operation whether said currently active linker or compiler program is found and

associated with said currently being handled file in said tables or not ;

determining legitimate if said active linker or compiler program was associated with said being handled file; otherwise

probing said proposed write operation whether said currently being handled file by said currently active application program is found(specified) and is not associated with said currently active application program in said tables or not in said tables;

determining illegitimate if said being handled file is found and is not associated with said currently active application program; otherwise

probing said proposed write operation whether said proposed operation is unlocking operation, an operation to file in read-write mode or an operation to file in read-only mode in said tables;

determining legitimate if said proposed write operation was unlocking or an operation to file in read-write mode or illegitimate and recording the decision with current time and date in a log file if said proposed write operation was an operation to file in read-only mode; otherwise

fetching privileged signal from keyboard and decoding;

determining legitimate if said privileged signal approved or illegitimate if disapproved.

4. The steps of claim 3 wherein said file in read-only mode comprising:

contents of said file and allocation information of said file in storage device.

5. The method of claim 3 wherein said being handled file by said current program is represented by extension of said being handled file.

6. A method for fetching privileged signal comprising:

a jumper line between keyboard IO port and a decoder decoding keyboard signals;

decoding said keyboard signals.

7. Another method for fetching privilege signal comprising:

fetching signal from keyboard IO port

8. The method of claim 6 is only used when this invention is embedded in a peripheral device.

9. The method of claim 7 is only used when this invention is embedded in main system.

10. The method of claim 7 wherein said privileged signal is invalid when said privilege signal is imitated by any other executable codes or program

11. The method of claim 7 wherein said privileged signal is valid if said privileged signal was only generated by a switch or keyboard stroke.

12. A system for protecting resource in storage device against computer viruses comprising:

means for initializing;

means for determining whether proposed write operation is legitimate or illegitimate based on currently active linker program, compiler program, application program, being handled file or mode of a current being handled file;

means for rejecting said write operation if said write operation is not legitimate;

means for forwarding said write operation to storage device if said write operation is legitimate;

means for reallocating contents of files in order to optimize access time to storage device;

means for attempting to recover faults occurred in conventional system;

means for diagnosing integrity of system;

means for disabling determining.

13. The system of claim 12 is embedded in peripheral device and a micro processor is used to execute program, ROM is used to contain said program and RAM is used to store symbols used by said program.

14. The system of claim 12 is alternatively embedded in main system.

15. The system of claim 12 is alternatively implemented as a system software and embedded in operating system.

16. A method for protecting resource in storage device against computer viruses as hereinbefore described with reference to drawings.

17. A system for protecting resource in storage device against computer viruses substantially as hereinbefore described with reference to the drawings.

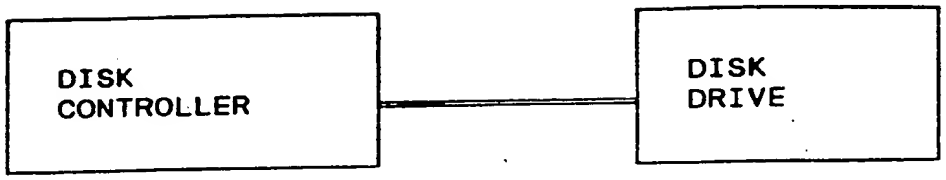

FIGURE 1

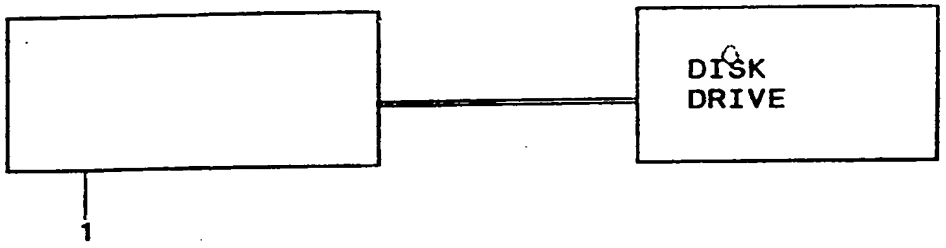

FIGURE 2

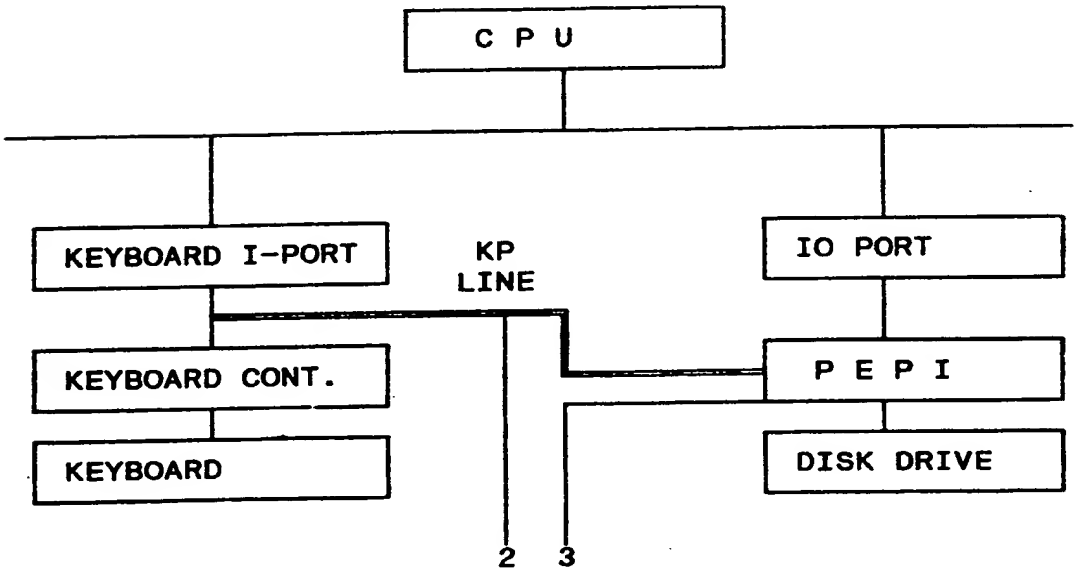

FIGURE 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR 92/00053

A. CLASSIFICATION OF SUBJECT MATTER

IPC[5]: G 06 F 12/14, 12/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC[5]: G 06 F 11/00, 12/14, 12/16

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

QUESTEL WPIL;
STN: INSPEC; PAT DPA

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO, A1, 91/13 403 (RODIME PLC) 05 September 1991 (05.09.91), see totality; especially claim 1; fig. 1.	1,12,16
A	GB, A, 2 231 418 (S & S Enterprises) 14 November 1990 (14.11.90), see pages 1,2.	1,12,16
A	GB, A, 2 222 899 (MORRIS ROSE) 21 March 90 (21.03.90), see totality.	1,12,16
A	DATABASE INSPEC (IEE) AN: 89:3325096, August 1988 TI: The brain virus	1,12,16

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 January 1993 (20.01.93)	27 January 1993 (27.01.93)

Name and mailing address of the ISA/ AT
AUSTRIAN PATENT OFFICE
Kohlmarkt 8-10
A-1014 Vienna
Facsimile No. 0222/53424/535

Authorized officer
MIHATSEK e.h.
Telephone No. 0222/53424/329

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR 92/00053

In Recherchenbericht angeführtes Patentdokument Patent document cited in search report Document de brevet cité dans le rapport de recherche	Datum der Veröffentlichung Publication date Date de publication	Mitglied(er) der Patentfamilie Patent family member(s) Membre(s) de la famille de brevets	Datum der Veröffentlichung Publication date Date de publication
WO A1 9113403	05-09-91	EP A1 516682 GB A0 9003890	09-12-92 18-04-90
GB A 2231418		GB A0 8910164 GB A1 2231418	21-06-89 14-11-90
GB A 2222899		AU A1 40995/89 GB A0 8919707 GB A1 2222899 US A 5144660 ZA A 8907831	08-03-90 11-10-89 21-03-90 01-09-92 26-06-91